SOPRA UNO SCRITTO IN CIFRA INTERPRETATO DA G. BATT. ARGENTI NEL 1581...

Emilio Benucci







SOPRA UNO SCRITTO IN CIFRA

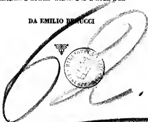
INTERPRETATO

DA G. BATT. ARGENTI

NEL 1581

MEMORIA ILLUSTRATA

DA EMILIO BERUCCI



ROMA

TIPOGRAFIA E LIBRERIA DI ROMA
DEL CAV. ALESSANDRO BEFANI
Via delle Stimate 23
1873.



Era un bel mattino di Ottobre, e Iacopo Boncompagni Duca di Sora nipote di Gregorio XIII allora regnante, stando a villeggiare nella sua deliziosa villa Tusculana, era visitato dal suo Maggiordomo Gio. Battista Argenti Romano, il quale sotto i Pontificati anteriori aveva servito come aiuto al Segretario delle cifre ed attendeva con passione a questi studii.

Il Duca, che pur si dilettava di Crittografia, aveva preparato, nell' ozio della villeggiatura, una piccola scrittura in cifra, onde tentare l' abilità del suo Argenti, e prender forse motivo di dargli piacevolmente la baia, insieme ai convitati, qualora non fosse riuscito alla soluzione.

Il documento onde ho ricavato tale anedoto esiste nella Biblioteca Chigiana. È un ricordo scritto di pugno dell'Argenti, che trascrivo esattamente

Qaetepeeeacszmddfictzadqgbpleaqtaiui

(In principio erat) questo è il motto o chiave con la quale l' Illmo ed Eccmo Sig. Iacomo Boncompagni Duca di Sora mio padrone ha scritto il soprascritto verso in cifra et datomelo il dì domenica 8. Ottobre 1581 in la Villa Tusculana dicendomi che non era possibile ritrovarla, et io li ho ritrovato subito subito la controcifra di X Alfabeti et il motto - Il verso soprascritto vuol dire et è questo

Arma virumque cano Troiê qui primus ab oris

A tergo poi del foglio medesimo sono notate queste parole « 1581 Cifra dell' Illo et Eccmo Sig. Padrone datami experiendi causa. 8 Octobris in Villa »

Conoscendosi il soggetto, la chiave, ed in genere anche il metodo tenutosi nel cifrare, è facile il dare la dimostrazione

Gli Alfabeti furono i seguenti:

Alfabeto 1.° AB	*a*	*b*	*c*	*d*	*e*	*f*	*g*	*h*	*i*	*l*
	m	*n*	*o*	*p*	*q*	*r*	*s*	*t*	*u*	*z*
» 2.° CD	*a*	*b*	*c*	*d*	*e*	*f*	*g*	*h*	*i*	*l*
	n	*o*	*p*	*q*	*r*	*s*	*t*	*u*	*z*	*m*
» 3.° EF	*a*	*b*	*c*	*d*	*e*	*f*	*g*	*h*	*i*	*l*
	o	*p*	*q*	*r*	*s*	*t*	*u*	*z*	*m*	*n*
» 4.° GH	*a*	*b*	*c*	*d*	*e*	*f*	*g*	*h*	*i*	*l*
	p	*q*	*r*	*s*	*t*	*u*	*z*	*m*	*n*	*o*
» 5.° IL	*a*	*b*	*c*	*d*	*e*	*f*	*g*	*h*	*i*	*l*
	q	*r*	*s*	*t*	*u*	*z*	*m*	*n*	*o*	*p*
» 6.° MN	*a*	*b*	*c*	*d*	*e*	*f*	*g*	*h*	*i*	*l*
	r	*s*	*t*	*u*	*z*	*m*	*n*	*o*	*p*	*q*
» 7.° OP	*a*	*b*	*c*	*d*	*e*	*f*	*g*	*h*	*i*	*l*
	s	*t*	*u*	*z*	*m*	*n*	*o*	*p*	*q*	*r*
» 8.° QR	*a*	*b*	*c*	*d*	*e*	*f*	*g*	*h*	*i*	*l*
	t	*u*	*z*	*m*	*n*	*o*	*p*	*q*	*r*	*s*
» 9.° ST	*a*	*b*	*c*	*d*	*e*	*f*	*g*	*h*	*i*	*l*
	u	*z*	*m*	*n*	*o*	*p*	*q*	*r*	*s*	*t*
» 10.° UZ	*a*	*b*	*c*	*d*	*e*	*f*	*g*	*h*	*i*	*l*
	z	*m*	*n*	*o*	*p*	*q*	*r*	*s*	*t*	*u*

Tali serie furono adoperate dal Duca secondo le regole della Crittografia nel modo seguente:

La prima lettera della chiave che è un I (In principio erat Verbum) determinò la serie ossia alfabeto che dovè sceglìersi cioè quello attergato IL che è il quinto. La prima lettera del tema è *a* (arma virumque ec.). Nella serie quinta alla lettera *a* corrisponde nella linea sottoposta un *q*: perciò il primo segno della cifra è *q*.

La seconda lettera della chiave è N, perciò si prese l'alfabeto MN che è il sesto. La lettera da mettersi in cifra è la 2. del tema cioè *r* (*a*rma) Alla *r* in detto alfabeto sesto corrisponde nella linea annessa un *a*. Dunque per secondo segno di cifra si pose *a*, e così di seguito.

Ecco lo specchio, nel quale, guardando verticalmente, si leggono e chiave, e tema, e cifra; mentre le orizzontali seguono i rapporti dei respettivi elementi.

A chi si diletta di tali studi piacerà peraltro andare un poco più oltre; misurare la difficoltà di questa cifra, indagare la via che verosimilmente avrà tenuto l'Argenti per venirne a capo, e così in conseguenza apprezzare il merito della soluzione.

Chiave	*Tema*	*Cifra*
I	A	Q
N	*r*	*a*
P	*m*	*e*
R	*a*	*t*
I	*v*	*e*
N	*i*	*p*
C	*r*	*e*
I	*u*	*e*
P	*m*	*e*
I	*q*	*a*
O	*u*	*c*
E	*e*	*s*
R	*c*	*z*
A	*a*	*m*
T	*n*	*d*
V	*o*	*d*
E	*t*	*f*
R	*r*	*i*
B	*o*	*c*
V	*i*	*t*
M	*e*	*z*
I	*q*	*a*
N	*u*	*d*
P	*i*	*q*
R	*p*	*g*
I	*r*	*b*
N	*i*	*p*
C	*m*	*l*
I	*u*	*e*
P	*s*	*a*
I	*a*	*q*
O	*b*	*t*
E	*o*	*a*
R	*r*	*i*
A	*i*	*u*
T	*s*	*i*

La cifra a prima vista poteva supporsi *anagrammatica*; ma per poco che si osservasse quello strano assortimento di lettere, dove tre *q* sono servite da una sola *u* si conosceva presto che non erano materiali acconci a formare parole in qualunque modo venissero riordinati. Quindi vi era trasformazione di caratteri.

Vedendo poi un gruppo di tre segni eguali *eee*, se ne inducova che non si trattava di una tramutazione semplice; poichè qualunque valore si assegnasse al segno *e*, non poteva una medesima lettera essere ripetuta congiuntamente per tre volte, salvo qualche caso rarissimo e non supponibile.

Si trattava dunque di una trasformazione complicata, nè l'Argenti avrà punto esitato a riconoscere la cifra degli alfabeti che era spesso per le mani dei dilettanti di crittografia.

Il metodo veramente è ingegnoso ed elegante, ma più adatto per esercizi accademici che per una seria corrispondenza secreta, riuscendo poco spedita la sua applicazione. Ne avea parlato il nostro italiano Gio. Battista Porta al Capo XVI del Libro II, nella sua bell' opera *De furtivis literarum notis vulgo de Ziferis*, che trovavasi impressa a Napoli pei tipi dello Scoto fin dal 1563. Benchè quell' autore non sia facile a vedere difficoltà, pure aveva detto « Est autem (hic astus) adeo involutus, ut, quamvis « etiam furtivi scripti species non lateat; neqnaquam sit « qui proprius eius cognoscendi modus intelligatur, fietque « potius ut quo magis eius perplexitatem quis explicare « conetur, eo magis interpretando ambiguus feratur ».

Coerentemente a questo criterio esposto nel Libro II si astenne il Porta nel libro III (che tratta del decifrare) dal dare alcun insegnamento circa la soluzione di tale cifra. Questo silenzio confermò che, a suo parere, la difficoltà era insuperabile, mentre al Capo IV del libro III avea fatta la sua protesta in questi termini « Duplex occultan- « di scripti genus esse, proximo volumine indicavimus; al- « terum quod adhibita diligentia, et certa ratione potest « interpretari; alterum quod Apolline solum aenigmatum

« auctore, no dicam Deo optimo Maximo interprete vide« tur indigere. Quare *hac parte intermissa*, illam prose« quamur. »

La ragione di tale difficoltà si vede chiarissima, perchè scomparsi tutt' i rapporti fra lo scritto e l'ortografia delle parole, sono subentrati i rapporti che hanno due dizioni incognite con un terza elemento convenzionale, cioè con le serie, che possono disporsi ad arbitrio.

Ma dunque, come potè accadere che un enigma di questa natura venisse sciolto *subito subito*, come ci ha lasciato scritto il buon Argenti? Sarà permesso di sospettare qualche reticenza circa i dati cogniti o un po' di millantazione? Nulla di ciò: Argenti era discepolo di Antonio Elio da Pola (1), che fu poi Patriarca di Gerusalemme e che per testimonianza del dotto contemporaneo *Vigenère* (Traitè des Chiffres pag. 35) non ebbe pari in valentia nell'arte. Forte perciò di un' eccellente scuola, e di un lungo esercizio, potè Argenti accettare la sfida, come potè trionfarne agevolmente atteso il concorso di alcune circostanze, che incontrò favorevoli alle sue ricerche, e che vado a porre in rilievo.

Infatti il Porta, se ben si osserva, espose la difficoltà cui può spingersi una tale cifra, non quella che di fatto si trovi sempre in ciascuna di esse. L' autore al libro 2.° trattava dei modi di scrivere occultamente, e perciò doveva segnalare in ognuno la forza occultativa, che ne forma il pregio. Prendete per base una filastrocca di lettere stranamente disposte fin dalla prima serie; adottate per chiave qualche barbara parola, componete la cifra, e poi ditemi se v'è chi possa disnodarla. Ma quando la struttura delle serie siegue l' ordine alfabetico e l' andatura consueta; in allora l'elemento, che era terribile per la sua variabilità, si avvicina alle condizioni di un dato cognito.

Il decifratore nelle sue congetture incomincia dalle combinazioni più normali, e nel caso nostro vi era una spe-

(1) Memorie di Matteo Argenti nipote di G. B. — Manoscritto nella Biblioteca Chigiana.

ciale ragione di farlo, non essendo supponibile che il cavalleresco Padrone avesse voluto sobbarcare l'indotta e fastidiosa briga di sconvolgere dieci alfabeti (con tutto il pericolo di errare nelle rotazioni) pel solo scopo di aumantare difficoltà, della quali si aveva sovrabbondanza anzichè penuria.

Ritenendo perciò che la disposizione della prima serie procedesse coll'ordine naturale, era da indagarsi di quante lettere si componesse, potendo farsi di 22 o di 20 come per lo più si pratica eliminandone due che pel latino sono l'*y* e lo *z*. Ma lo *z* figura due volte nella cifra, mentre *x* e *y* non vi si trovano affatto. Da ciò potè arguire Argenti che le lettere fossero 20, gli Alfabeti 10, che l'*x* e l'*y* fossero escluse e che la tabella fosse predisposta in conseguenza nel seguente modo:

a b c d e f g h i l
m n o p q r s t u z

La struttura normale della serie fu la prima circostanza favorevole alla soluzione del problema.

Restava ora a vedere in qual modo succedeva la rotazione, se da destra a sinistra, o viceversa, e se saltuariamente, o serbando anche in ciò l'ordine alfabetico. Argenti che aveva tanta famiharità colle cifre, da poter dire come disse Tullio degli ameni studii letterarii *pernoctant nobiscum, peregrinantur, rusticantur*; superò facilmente quest' ostacolo. Egli ben sapeva che ritenuto il contingente della prima serie nel modo indicato, comunque poi si regoli la rotazione, è imprescindibile che ad ogni lettera fissa (*a b c d e f g h i l*) corrisponda una colonna composta delle mobili (*m n o p q r s t u z*) e viceversa, in continuo antagonismo; quindi mi par di vederlo quando in un brano di carta vergava le seguenti note

Q	*a*	*e*	*t*	*e*	*p*	*e*	*e*	*e*	*a*
a	*m*	*m*	*a*	*m*	*a*	*m*	*m*	*m*	
b	*n*	*n*	*b*	*n*	*b*	*n*	*n*	*n*	
c	*o*	*o*	*c*	*o*	*c*	..	..	..	
d	*p*	*p*	*d*	*p*	*d*	..	..		
e	*q*	*q*	*e*	*q*	*e*	..			
f	*r*	*r*	*f*	*r*	*f*				
g	*s*	*s*	*g*	*s*	*g*				
h	*t*	*t*	*h*	*t*	*h*				
i	*u*	*u*	*i*	*u*	*i*				
l	*z*	*z*	*l*	*z*	*l*				

dove, come ognuno vede, sono intestati i segni della cifra e nella respettiva colonna sono disposti verticalmente tutti i valori di cui quel segno è suscettibile senza punto occuparsi del motto servito per chiave.

Or si accinge a passare in rassegna le combinazioni delle lettere fra di loro, ed incominciando dall' *a* della prima colonna colla lettere dalla seconda, e scegliendo le migliori a più frequenti formazioni, ottiene

am - an - ar - as - at

Congiungendo queste sillabe agli elementi della colonna terza, e spigolando sempre il meglio, prende appunto dalle seguenti

amn	*ann*	*arm*	*ast*	*at-m*
	ant	*ars*		*at-n*
	an-p	*art*		*at-p*
	an-s			

Ma eccolo già sul punto di entrare in quello spinaio tanto magistralmente descritto dal Porta, dove l' interprete tanto più s' intrica quanto più s' inoltra; eppure egli prosiegua! Dio glie la mandi buona.

Occorre assolutamente una vocale, e la quarta colonna glie ne può dar trè *a e i*. Incomincia dall' *a* ad aggregandola alle combinazioni anteriori gli risultano

Anna
Anta
An-pa (con separazione di parole)
An-sa id.
Arma

Chi non vede che fra queste combinazioni l' ultima è la più probabile? Questa richiama il notissimo verso primo dell' Eneide. Argenti vi si ferma, lancia un'occhiata alle colonne successive per vedere se vi sono i materiali acconci a dare la *u*, la *i*, la *r* ecc. per formare *virumque*, e li scorge opportuni: in men che non si dice ha già dispiegato il verso sotto la cifra in tutta la sua estensione e dalle parole del soggetto poste a fronte della cifra viene fuori anche il motto adoperato per chiave. Argenti hai vinto. Va pure a raggiungere la brigata che passeggia negli ombrosi viali della villa, od avrai le meritate congratulazioni.

L' essersi scelto per soggetto il notissimo verso Virgiliano, fu, come ognun vede, l' altra circostanza favorevole che decise della vittoria. Nell' affaticarsi della mente verso la scoperta dell' occultata scrittura si presentano per prime le rimembranze degli studi giovanili, le sentenze più note, i detti più celebri. Lo sperimentò l'istesso Porta, e molto opportunamente ne fece menzione al citato Capo XVI del secondo libro, ove disse: « Huius loci est referre superioribus diebus in hunc modum missam epistolam a scio« lo quodam, qui Romae agebat, cum eius admiratione, « eadem hora, qua litteras accepi, me fuisse interpreta« tum; cuius rei causa fortasse esse potuit quod index « scripti hoc erat *Omnia vincit amor* quae sententia, pro« verbii vice, nemini fere non cognita est. »

Che se riesce comoda la notorietà della chiave ossia indice, molto più sarà vantaggiosa la notorietà del sog-

getto, sia perchè quello è *mezzo* e questo è *fine*, sia perchè l'indice è dei tre elementi il più rinserrato e rimoto, giacchè impiegate per il primo nel lavoro della sintesi, è regolarmente l'ultimo a venir fuori nel processo dell'analisi.

Potrebbe obbiettarsi che quella successione di tentativi da me supposta non è un metodo scientifico, e che sarebbe stato più conforme alle teorie il prender di mira i tre segni eguali e congiunti *e e e*, il mettersi alla caccia delle lettere *q* ed *u* che sono inseparabili, il forzare la finale ecc. Convengo; ma per coordinare queste indagini si richiedeva un lavoro un po' lungo, e qui faceva d'uopo disbrigarsi: bene o male che ne venisse, bisognava andar per le corte.

Nelle memorie storiche sull'arte di decifrare, che ordinariamente sono premesse alla parte tecnica, dagli autori che ne trattano, poco o nulla si parla del nostro paese. L'aneddoto di Villa Sora, prescindendo da altri e più serii documenti, è una prova che questo studio, fin da tre secoli fa, era coltivato con profitto dagl'Italiani.



